(12) Japanese Unexamined Patent Application Publication

(11) Publication No. 2000-4482

(43) Publication Date: January 7, 2000

(21) Application No. 10-170366

(22) Application Date: June 17, 1998

(71) Applicant: Nippon Telegraph and Telephone Corp., 3-1, 2-chome, Ohtemachi, Chiyoda-ku, Tokyo

(72) Inventor: Tetsutada SAKURAI
c/o Nippon Telegraph and Telephone Corp., 19-2, 3-chome, Shinjyuku, Tokyo

(72) Inventor: Teruo HAGINO
c/o Nippon Telegraph and Telephone Corp., 19-2, 3-chome, Shinjyuku, Tokyo

(72) Inventor: Yoshitake SUZUKI
c/o Nippon Telegraph and Telephone Corp., 19-2, 3-chome, Shinjyuku, Tokyo

(72) Inventor: Yutaka NISHINO
c/o Nippon Telegraph and Telephone Corp., 19-2, 3-chome, Shinjyuku, Tokyo

(74) Agent: Patent Attorney, Masatake SHIGA

(54) [Title of the Invention] PHS POSITION-INFORMATION NOTIFYING SYSTEM

(57) [Abstract]

[Object] To provide a PHS position-information notifying system that does not permit position information to be illegally acquired between a position-detecting client terminal and a detection-target terminal.

[Solving Means] Upon finding line connection made from a client terminal (S1), a position-information converting center 4 determines whether the client terminal is a service-contractual registered terminal (S2) for authentication. Subsequently, when logging-in is received from the client terminal (S3), the position-information converting center 4 performs user authentication (S4); in response to a detection request for a detection-target terminal 1 (S5), it performs terminal-calling to a network 5 (S6); and it issues a position-information notification request to the detection-target terminal 1 via the network 5 (S7). The detection-target terminal 1 includes encrypted position information in a call specification and transmits it to the position-information converting center 4 via the network 5 (S8 and S9). Then, steps S10 to S17 are performed between the position-information converting center 4 and the detection-target terminal 1; and the position-information converting center 4 encrypts latitude/longitude information corresponding to the position information and transmits the encrypted information to the client terminal (S18).

[Claims]

[Claim 1] A PHS position-information notifying system in a communication system wherein a detection-target terminal performs detection of information specifying a communicating PHS radio base station and performs notification to a position-information converting center, and a client terminal detects the detection-target terminal and/or inquires about the position thereof from the position-information converting center, characterized in that the position-information converting center comprises authenticating means for restricting the client terminal that is permitted to detect detection-target terminal and to acquire the position information thereof to a predetermined terminal.

[Claim 2] A PHS position-information notifying system according to Claim 1, characterized in that the authenticating means restricts the client terminal to at most two terminals including a backup terminal.

[Claim 3] A PHS position-information notifying system according to one of Claims 1 and 2, characterized in that a call-communication destination for the detection-target terminal is limited to that set to a predetermined single number.

[Claim 4] A PHS position-information notifying system according to one of Claims 1 to 3, characterized in that the

position-information converting center is connected by cable to the client terminal.

[Claim 5] A PHS position-information notifying system according to one of Claims 1 to 4, characterized in that the detection-target terminal comprises means for performing encryption/decryption of information communicated with the PHS radio base station or the position-information converting center, the encryption/decryption being performed by using common-key cryptograms or public-key cryptograms transmitted using public keys.

[Claim 6] A PHS position-information notifying system according to one of Claims 1 to 5, characterized in that the position-information converting center comprises converting means for receiving information specifying the PHS radio base station and for converting the information into latitude/longitude information, and means for encrypting information including at least the latitude/longitude information converted by the converting means and for transmitting the encrypted information to the client terminal.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention] The present invention relates to a PHS position-information notifying system in which information corresponding to a position of a portable

communication apparatus (detection-target terminal) using PHS (personal handy-phone system) radio communication (the information will be referred to as "position information" hereinbelow) is converted into latitude/longitude information, and the converted information is notified to a position-detecting client terminal. More particularly, the invention relates to a PHS position-information notifying system in which a detection-target terminal is used to thereby transmit the position information of the detection-target terminal to a position-information converting center; the position-information converting center converts the transmitted position information into latitude/longitude information and then performs notification thereof to either a terminal-position monitoring terminal or a position-detecting client terminal; and either the terminal-position monitoring terminal or the position-detecting client terminal correlates the position of the detection-target terminal with a map, an address, or the like; and management of the information is thereby performed.

[0002]

[Description of the Related Art] Existing communication apparatuses using PHS radio communication include an apparatus for transmitting the position information regarding the location of the communication apparatus. They also include an apparatus of which the position is a target

of an inquiry (that is, the aforementioned detection-target terminal). There are companies providing services for distributing the aforementioned information. An example of such services is "Ima-doko (or where are you now) Service" provided by NTT Chuo Personal Network K.K. Timing with which the detection-target terminal transmits the information is determined in two ways. In one way, notification is performed in response to each instruction transmitted from the monitoring center (the instructions include those issued based on user requests transmitted from the position-detecting client terminal). In the other way, notification is performed using a function that is preset in the detection-target terminal to be activated according to set time, periods, or the like.

[0003] FIG. 4 schematically shows the relationship among communication terminals used in the above-described service and a center apparatus that functions as a core of the service. In the figure, reference numeral 1 denotes a detection-target terminal for which a terminal, such as a PHS telephone or a dedicated-card-type terminal equivalent thereto, is used. According to a protocol of a PHS telephone system, the detection-target terminal 1 detects a base station with which it can communicate at a position where the detection-target terminal is located in response to either a random call or a periodical call from a close

base station 2 (which may be referred to as a "CS", as shown in the figure). Then, it performs notification of an identification number of the base station (which hereinbelow will be referred to as a "CS-ID"). A series of these information transmission operations uses a radio wave determined according to the PHS telephone system. Therefore, the base station 2 that can receive the information transmitted through the notification is restricted to be located close or within a radius of about 100 to 500 m with the detection-target terminal 1 in the center. Even in a case where a plurality of such base stations exist, accessible base stations are limited to those located close to the detection-target terminal 1. In addition, information regarding CS-IDs and installation sites of the base stations are totally managed by a position-information converting center 4. Therefore, when a CS-ID number received in association with an ID number of the detection-target terminal 1 is identified, a spot close to the position of the detection-target terminal 1 can be identified.

[0004] In addition to the above-described steps, operation of a PHS telephone system for which the radio-wave transmission intensity is increased is also performed. In this case, since the detection-target terminal receives radio waves from a plurality of base stations in a single

step, difficulty in specifying a close base-station antenna may arise. As a measure to overcome such difficulty, operations corresponding to the radio-wave reception intensity are experimentally performed to detect the position. These operation steps are executed such that received CS-IDs of base stations are read and associated with latitude/longitude information, and the radio-wave reception intensity is used as "weight" for each of the base stations. Then, the center of the weight of a polygon formed with the base stations as vertexes is obtained to thereby identify a spot close to the position of the detection-target terminal. Methods that are experimentally used also include a method in which two vertical lines each perpendicularly bisecting a line segment connecting two base stations of which the radio-wave reception intensities are substantially the same are obtained, and the intersection point thereof is determined to be a spot close to the position of the detection-target terminal.

[0005] Thus, the position of a detection-target terminal can be identified at a practical level according to the above-described principles. The position-information services using the PHS telephone system have been practically used since the spring of 1998. For example, the services have been practically used in, for example, cases where parents anxiously waiting at home for their child to

return home make an inquiry for position information and cases where a party can obtains the behavior of groups of students in free-activity time on an excursion trip or the like without accompanying them.

[0006] In FIG. 4, a position-detecting client 3 may be a personal computer, a workstation, or any device capable of transmitting information for specifying a detection-target terminal for detection. For example, a facsimile machine and an ordinary telephone are used in addition to a personal computer in a position-detecting service that has been used since the autumn of 1997 in Sakata-city in Yamagata Prefecture for aged people who tend to roam about. In this case, to specify a detection-target terminal through the facsimile machine and the telephone, the number of the detection-target terminal is input using pushbuttons of the facsimile machine or the telephone. For a network 5 in FIG. 4, an ISDN (integrated services digital network) or the like is used.

[0007] Hereinbelow, steps of an existing position-information service will be explained in detail. In the system configuration and service schematically illustrated in FIG. 4, a detection request for the position information of the detection-target terminal 1 is issued to the position-information converting center 4 via the network 5 from the position-detecting client 3 (step 1). Upon receipt

thereof, the position-information converting center 4 issues a position-information notification request to the detection-target terminal 1 via the network 5 and the base station 2 (step 2). The detection-target terminal 1, at its present location, detects a base station 2 with which it can communicate, and returns a CS-ID of the base station to the position-information converting center 4 via the network 5 (step 5). Since the position-information converting center 4 preliminarily has a table in which site-position (latitude/longitude) information is correlated to the received CS-ID of the base station, it immediately reads the information and associates it with latitude/longitude information (step 4). Subsequently, the position-information converting center 4 delivers the latitude/longitude information to the position-detecting client 3 via the network 5. The position-detecting client 3 combines the information with map information which is stored separately, thereby enabling a CRT (cathode ray tube) to display the position of the detection-target terminal 1 (step 5).

[0008] In a configuration in which a facsimile machine is used for the position-detecting client 3, a facsimile signal is used to transmit a notification from the position-information converting center 4 to the position-detecting client 3. Thereby, the notification can be displayed in the

form of a facsimile image. Also, in a configuration in which a telephone or the like is used for the position-detecting client 3, the position-information converting center 4 converts the site-position information into speech (an example is "The inquired terminal is located at $$ (lot number), @@-cho (town), ##-ku (block), **-shi (city)), thereby enabling output of speech from the telephone.

[0009] Hereinbelow, referring to FIG. 5, a detailed description will be given regarding acquisition of position information when a user moves. In FIG. 5, individual portions are illustrated placing first priority on easy viewing, and the same configuration portions as those in FIG. 4 are shown with the same reference numerals or symbols. Reference numerals such as 21, 22, and 23 in FIG. 5 each denote a base station equivalent to the base station 2 shown in FIG. 4; and reference numerals 6, 6, ... 6 denote a CS interface section for managing the base stations. An ISDN and a control system 7 correspond to the network 5 shown in FIG. 4; and the CS interface sections 6 are connected thereto. In addition, a PHS telephone system is configured to include detection-target terminals 1 of individual users (the moved detection-target terminals 1 are designated with 1a, 1b, etc.), and a plurality of terminals (not shown). The PHS telephone system provides PHS telephone services that will be described below.

[0010] In the PHS telephone system, not only the inter-PHS communication service, but other networks (such as, a PSTN (public switched telephone network) or Internet, which are not shown) are connected or can be connected. In addition, communication can be made with ordinary domestic telephones. Furthermore, a position-information service which is within the field of application of the present invention has recently been added. The description given below covers services and systems other than those with telephone services. Therefore, in the description, the PHS telephone service is referred to as the "PHS service", and the PHS telephone system is referred to as the "PHS system".

[0011] As described above, the PHS service includes a variety of services that can be executed. The PHS service is a personal-use communication service in which radio waves of a 1.9 GHz band are used; radio-frequency (which hereinbelow will be referred to as "RF") outputs of at most 10 mW are produced from portable terminals, outputs of at most 500 mW (the output value can be controlled according to the coverage of an intended base station) are produced from public stations (i.e., the base stations 21, 22, 23, etc.); and voice or digital data of up to 32 kbits/s per slot is communicated. In addition, in the PHS system, time slots (625 μs/slot) for communication to be made in 5-μs unit times called TDMA/TDD (time-division multiple access/time-

division duplexing) frames are allocated, and a voice channel for three terminals is provided for one base station. A "control channel" for controlling the voice channel is provided between one base station and the three channels. As a matter of course, these numbers are applied to the existing example cases and can therefore be changed according to socially required technological developments in the future. Even in the future, it should be apparent that the primary concept of the present invention would not be impaired.

[0012] The PHS service used with a telephone tolerates a low-speed motion. (Motion which is made at a speed of 30 km/h or lower. However, since the speed of motion depends upon the cell capacity, it slightly varies depending upon the company that provides the PHS service. Hereinbelow, the speed of motion will be referred to as a "predetermined PHS tolerance speed".) Therefore, the system must always store data of positions of user terminals. Hereinbelow, this function will be shortly described referring to FIG. 5. Areas where radio waves transmitted from the base stations 21, 22, and 23 can be received are individually represented by cells C1, C2, and C3. Areas where radio waves transmitted from other base stations (not shown) can be received are individually represented by cells C4, Cx, Cy, etc. It is assumed that the detection-target terminal 1

initially stays in the cell C1, and then sequentially moves to the other cells, such as the cell C2 and the cell C3 (As described above, the moved terminals are shown as the detection-target terminals 1a and 1b). Also, as described above, in addition to the detection-target terminal 1, a plurality of detection-target terminals (not shown) is assumed to exist.

[0013] Positions of a large number of the terminals are each identified and recorded (the recording operation is referred to as "position registration", hereinbelow). In this state, if an accessible base station is registered each time a terminal moves, radio-wave congestion is caused. To prevent this, a step called "general calling" is performed. The general calling is performed such that a plurality of public base stations is grouped to form a position registration area (For example, the cell C1 and the cell C2 form one position registration area); position registration of PHS terminals such as the detection-target terminals 1 is not performed in units of the public base station, but is performed only when the position registration area is changed; in reception operation, each of the plurality of public base stations in a position registration area in which PHS terminals can exist perform calling to the PHS terminals; and only public base stations that have received a response perform the reception operation for that PHS

terminal.

[0014]

[Problems to be Solved by the Invention] In the above-described steps, measures are taken to prevent illegal radio interception and position-information acquisition. For example, in information communication between a public base station and a PHS terminal, ordinary cryptographic communication is employed; and steps, such as cipher-key establishment, authentication requesting, and authentication responding, are performed therein. Therefore, it is difficult to perform radio interception to thereby illegally acquire the position information. In transmitting (making a call for) a position-detection request from the position-detecting client 3 (or a telephone or a facsimile machine that has an equivalent function) to the position-information converting center 4 in the configuration shown in FIG. 4, a series of steps, such as authentication requesting, authentication-number input, personal-identification-number requesting (the personal identification is also called a password), and personal-identification-number input, are performed to enhance security.

[0015] Despite the fact that the security is taken into consideration, when the overall system is viewed with respect to robustness, it still has portions that need to be improved. The primary portion is a user interface. FIG. 6

shows steps of an ordinary PHS service. As shown therein, two-staged steps are carried out to protect access from a terminal such as a position-detecting client 3 ("terminal-position monitoring center or requesting terminal" in the figure) to a position-information converting center 4. One of the steps is access-line authentication ("connection-line authentication" in the figure), and the other step is access-user authentication (shown as "user authentication" in the figure).

[0016] In the line authentication, however, the security can perhaps be broken by an illegally acquired portable terminal which is permitted to access the position-information converting center 4. Also, although a password is used as a guard in the user authentication, in practice, a case can occur in which a malicious third party acquires a personal identification required to request the detection of position information. Such cases can occur because a simple alphabetical string or a numerical string is easily selected for the password, which needs to be memorized by a user, to avoid input errors. Typical examples using a numerical-string password include a bank cash card. For the password, a user tends to use a numerical string representing his or her birthday or a postal code that can be easily known by third parties. Therefore, security with such a password can be easily broken. This is apparent from the fact that cash

is frequently withdrawn using illegally acquired cash cards. As it is apparent from this fact, personal information that should be protected for privacy and the location of valuables can be easily known to malicious third parties.

[0017] The present invention is made in view of the above problems. An object of the invention is therefore to provide a PHS position-information notifying system used in a communication system that detects information and a reception-signal level which are used by a detection-target terminal to designate a PHS radio base station and notifies the information from a position-information converting center to a position-detecting client terminal, the PHS position-information notifying system being provided with a security between a terminal to which position information is notified and the detection-target terminal so as not to permit a malicious third party to illegally acquire the position information.

[0018]

[Means for Solving the Problems] To solve the above-described problems, the invention as described in Claim 1 is a PHS position-information notifying system in a communication system wherein a detection-target terminal performs detection of information specifying a communicating PHS radio base station and performs notification to a position-information converting center, and a client

terminal detects the detection-target terminal and/or inquires about the position thereof from the position-information converting center, characterized in that the position-information converting center comprises an authenticating means for restricting the client terminal that is permitted to detect detection-target terminal and to acquire the position information thereof to a predetermined terminal. The invention as described in Claim 2 is a PHS position-information notifying system characterized in that in the invention as described in Claim 1, the authenticating means restricts the client terminal to at most two terminals including a backup terminal. The invention as described in Claim 3 is a PHS position-information notifying system characterized in that in the invention as described in one of Claims 1 and 2, a call-communication destination for detection-target terminals is limited to that set to a predetermined single number. Specifically, a call-communication destination for the detection-target terminals is limited to a predetermined single number closely related to the client terminal. The single number is selected from numbers of telephones set in a room in which the client terminal is placed and numbers at which communication can be made with personnel managing the detection-target terminals.

[0019] The invention as described in Claim 4 is a PHS position-information notifying system characterized in that

in the invention as described in one of Claims 1 to 3, the position-information converting center is connected by cable to the client terminal. The invention as described in Claim 5 is a PHS position-information notifying system characterized in that in the invention as described in one of Claims 1 to 4, the detection-target terminal comprises a means for performing encryption/decryption of information communicated with the PHS radio base station or the position-information converting center, the encryption/decryption being performed by using common-key cryptograms or public-key cryptograms transmitted using public keys. The invention as described in Claim 6 is a PHS position-information notifying system characterized in that in the invention as described in one of Claims 1 to 5, the position-information converting center comprises a converting means for receiving information specifying the PHS radio base station and for converting the information into latitude/longitude information, and a means for encrypting information including at least the latitude/longitude information converted by the converting means and for transmitting the encrypted information to the client terminal.

[0020]

[Embodiments] Hereinbelow, referring to the drawings, an embodiment of the present invention will be described.

First, an outline of the present invention will be described. The present invention is a PHS position-information notifying system. In the system, a detection-target terminal to which an inquiry about position information is is associated either with a terminal-position monitoring terminal that makes the inquiry or with a position-detecting client terminal not to allow an inquiry made from a source other than the associated terminals to be authenticated. Therefore, a dedicated mutual authentication relationship is established between the detection-target terminal and the position-detecting client terminal or the like, thereby providing a function to reject an illegal third-party intervention. In addition to the mutual authentication, the present invention provides a function that allows position information to be encrypted for communication. Therefore, even when a third party attempts to illegally access the system, he/she is not permitted to accomplish their purpose.

[0021] FIG. 1 illustrates example position-information detection steps according to the embodiment. The steps will be described later in detail. Meanwhile, a description will be made primarily regarding differences from the conventional example. A first aspect significantly different from the above-described conventional example (refer to FIG. 6) is that a client terminal permitting detection of a detection-target terminal 1 and acquisition

of the position information thereof is restricted. Specifically, in the present embodiment, the position-detecting client 3 shown in FIG. 4 is restricted only to a specific terminal designated at the time of conclusion of a position-information service contract (that is, a "service-contractual registered terminal" shown in FIG. 1). For the restriction level, preferably, only one client terminal may be used, and the client terminal is connected by a cable. This is preferable because it can easily be checked whether wire-tapping is performed for cable-connected items. In practice, a backup client terminal is set to prepare for unexpected incidents, such as malfunctions. In the configuration, a function may be added such that transmission can be performed to a specific single number from a detection-target terminal. The single number is set to a number with which connection can be made from a detection-target-terminal possessor either to a client-terminal operator or to a detection-target-terminal administrator. In this way, a single terminal possesses the reception number used for receiving information from the detection-target terminal.

[0022] A plurality of terminals other than the detection-target terminal 1 shown in FIG. 4 may be included in the system. This configuration, of course, is included in the scope of the invention. Also, the configuration may include

a PHS service system configured of a plurality of groups each consisting of at most two client terminals, including a backup terminal, and a plurality of detection-target terminals. This configuration is also included in the scope of the present invention. In this case, however, detection by a client terminal belonging to a group for a terminal belonging to a group different from the aforementioned group is out of the purpose of the present invention. To prevent such an operation, systematic security is provided. Specifically, the series of steps described in the beginning of "Problems to be Solved by the Invention" is carried out.

[0023] The level of the quality of services provided by the system, in which the client terminal permitted to obtain the position information or to issue detection requests is thus restricted, tends to be considered to be lower than quality of the conventional service that allows any terminal to use the position-information service as long as it presents a correct password. However, as it becomes apparent through careful consideration, the system of the embodiment is preferable since confusion that can occur in the case of emergency can be eliminated. The confusion can be eliminated by the configuration built such that the client terminal that should totally control position information, which is changeable from time to time, is either allocated to a restricted person or set at a restricted site. In

addition, connection numbers (i.e., terminal identification numbers, such as a connection telephone number, a facsimile number, a mail address, and a URL (uniform resource locator)) thereof are restricted.

[0024] In addition, for the telephone that performs transmission only to specific numbers, a PB (push button) function as provided in a PHS service can be avoided. Therefore, the detection-target terminal can be fabricated to be light and at a lower cost, and operation to be performed by a user possessing the detection-target terminal 1 can be simplified. Also, (since only designated terminals are permitted to perform reception), the system can prevent illegal overuse of the service by malicious third parties who illegally acquired a detection-target terminal. Thus, it is apparent that significant advantages that are not available in the existing services with telephones and PHS terminals can be obtained. Actually, the inventors implemented transmission of information to and reception thereof by using a number designated by a pilot system in a manner of using a specific push-button pushing pattern different from an ordinary power-button pushing pattern. In practical services, however, it is more realistic than the above to make the arrangement such that a power-on/off operation is performed using a predetermined power-button operation to thereby enable reception or

response to be performed by a single push operation of the power button.

[0025] A second feature of the present embodiment is that cryptograms are used for transmitting information from the position-information converting center 4 to a service-contracting registered terminal (i.e., the information including latitude/longitude information of the position where the detection-target terminal 1 is located, and an ID number or a telephone number of the detection-target terminal 1). In recent years, various types of encryption algorithms and systems have been proposed and are used. Typical examples include processing-speed oriented FEAL (fast encryption algorithm)-8 and RC5, each of which is called a common-key cryptosystem; and public-key cryptosystems MISTY and SQUARE, which are restricted in processing speed, which are characterized by high security. However, when one of these cryptosystems is used, it is difficult to simultaneously satisfy two requirements, one for security (robustness) and the other for information transmission without causing much delay.

[0026] However, in the present embodiment, an encryption application field is restricted to text representing "latitude/longitude information regarding the position of the detection-target terminal and an ID number of the detection-target terminal". In this case, the information

can be represented by a short numerical string or an alphabetical string. Therefore, the embodiment can employ a public-key cryptosystem, which is not suitable to a long character string, but has high robustness. Specifically, the position-detecting client 3, which is the application object of the present embodiment, has encrypting keys and decrypting keys of the public-key cryptosystem in itself and the position-information converting center 4, thereby allowing high-security communication to be easily performed only to a predetermined receiving party. Also, as an application thereof, a method can be employed such that public encryption keys are transmitted by using the public-key system to thereby perform communication of a long character string or long communication in a realistic processing period of time. This method provides a significant advantage in that the aforementioned wire-tapping in communication in the cable connection finishes unsuccessfully. As a matter of course, even when a malicious third party accesses the position-information converting center 4, all efforts it has exerted result in failure. From this viewpoint, it is very important to provide the position-information converting center 4 in a security-protection area of an intranet.

[0027] FIG. 2 schematically shows a practical example configuration of a portable terminal according to the

present embodiment. A portable terminal 100 has the following configuration. A microantenna 101 works as an interface for transmitting and/or receiving PHS-standard radio waves, and is formed of a ceramic antenna chip or the like. A radio section 120 processes PHS-standard radio waves transmitted and/or received via the microantenna 101. It includes a radio control section 102, a cryptographic processing section 103, a CS-ID detecting section 104, and a signal-level detecting section 105. The radio control section 102 controls transmission and reception of PHS-standard radio waves, which are performed via the microantenna 101. When signals included in PHS-standard radio waves received by the radio control section 102 are encrypted, the cryptographic processing section 103 decrypts the encrypted signals. In addition, the cryptographic processing section 103 encrypts information transmitted from a control section 106 according to an instruction issued by the control section 106 and transmits the encrypted information from the microantenna 101 via the radio control section 102. The CS-ID detecting section 104 detects CS-IDs sent from signals decrypted in the cryptographic processing section 103 and transmits the detected signals to the control section 106 (which will be described below). The CS-IDs can thus be known. In this way, the processing steps are implemented under the control of the control section 106.

On the other hand, the signal-level detecting section 105 analyzes the intensities of PHS-standard radio waves to thereby perform tuning for the radio control section 102 to enable the most appropriate signal reception.

[0028] The control section 106 performs overall control in the portable terminal 100, including control of energy consumption. In addition, a PHS basic function section 107 primarily controls call-communication. Therefore, it is preferable that the control function of the control section 106 and the PHS basic function section 107 be an independent module (function). This is because, in many cases, the control including the control of energy consumption in the entirety of the portable terminal 100 differs from the control of call-communication service functions using the PHS system. It is advantageous that a so-called RISC (reduced instruction set computer) chip is used for the former control function, and a DSP (digital signal processor) is used for the latter control function. However, these requirements are not indispensable since a chip having both functions has recently been developed according to the concept of a system LSI (large-scale integrated circuit). As a matter of course, the practical usability of the system is increased by making the arrangement such that the PHS basic function section 107 primarily performs the call communication, and in addition, a module such as the control

section 106 is included so as to suitably function for the position-information service or the position-detecting service, both of which are included in the application field of the invention.

[0029] In addition, the inventors preliminarily performed experiments and learned that management of notification logs is the most important. Therefore, the embodiment contains a module having a function therefor. The module includes a notified-information recording section 108 for overall management of notified information, a notification-period/notification-time recording section 109 for storing data of periods or time that are used for position-information notification, a position-information-acquisition-period recording section 110 for storing periods in which position information such as CS-IDs and the like transmitted from public radio stations are obtained. The PHS basic function section 107 compares newly received CS-ID information with position-information notification logs stored in the notified-information recording section 108, and performs position-information notification upon finding a variation in the CS-IDs. When the detected CS-ID is of a single type, the terminal is moving and is located at a place where radio waves do not reach, such as a place near the end of a base-station service area or a place in a building. As the above state continues, with subsequent

position-information notification as a turning point, the radio-wave quality may be significantly degraded to such an extent that notification is disabled. However, before the terminal enters such a state where such an incident occurs, the PHS basic function section 107 notifies a base station or the like of preventive status information.

[0030] Thus, even users, such as the aforementioned elderly people who tend roam about and are not skilled at operation of the portable terminal 100, the notified-information recording section 108, the notification-period/notification-time recording section 109, and the position-information-acquisition-period recording section 110, can receive the PHS position-information services without an operational burden being imposed on them. With timing recorded in these recording sections, position information is automatically transmitted to the position-information converting center 4 via the network 5. In FIG. 2, reference numeral 111 denotes a battery for supplying power to the individual sections of the portable terminal 100. Reference numeral 112 denotes a power switch formed of the above-described power button and the like.

[0031] Hereinbelow, referring to FIG. 3, a detailed example configuration of a position-information converting center (refer to FIG. 4) will be described. As shown in the figure, a position-information converting center 115 of the present

embodiment communicates information with the base station 2 shown in FIG. 4 (or, the base stations 21, 22, 23, etc. in FIG. 5) and the position-detecting client 3 via an ISDN 116 (equivalent to the network 5 in FIG. 4), which is an infrastructure of the PHS services. A CS-ID which has been transmitted from the base station via the ISDN 116 cannot be used in the position-information service. Therefore, according to processing in the individual sections described below, the transmitted CS-ID is converted into latitude/longitude information.

[0032] A circuit interface section 118 is an interface for controlling communication with the ISDN 116. In this embodiment, since the circuit interface section 118 plays an important role, attention needs to be directed thereto. Specifically, since cipher-signal communication is not a prerequisite for the ISDN network, basic information such as telephone numbers identifying call-communication sources or call-communication destinations cannot be encrypted. Therefore, until the initial step of specifying a call-communication destination/call-communication source is completed, and a so-called telephone-line connection is established, the circuit interface section 118 functions as an ordinary circuit interface; and immediately before communication of information is started with a call-communication destination, the circuit interface section 118

passes process control to a cryptographic processing section 117. Only for ordinary call communication, as practical selection, the cryptographic processing may be passed to scramble processing in the PHS service instead of the cryptographic processing section 117

[0033] The cryptographic processing section 117 detects a CS-ID transmitted from the base station via the ISDN 116. When the CS-ID is encrypted, it decrypts the encrypted code and passes the result to a position-information converting section 121. Based on a conversion table (in the form of a file or records for reading CS-IDs, which are pieces of base-station information, and for associating with corresponding latitude/longitude information) stored in a base-station-information recording section 122, the position-information converting section 121 reads the CS-ID passed from the cryptographic processing section 117 as latitude/longitude information of the CS-ID. Then, the position-information converting section 121 transmits an alphanumeric string representing the obtained latitude/longitude information to the circuit interface section 118. The aforementioned cryptographic processing section 117 adds an ID number and the like of the detection-target terminal 1 to the latitude/longitude information that is to be transmitted via the circuit interface section 118. Subsequently, the cryptographic processing section 117

encrypts these pieces of information and transmits the encrypted information to the position-detecting client 3 via the ISDN 116. As shown in the figure, the position-information converting section 121 and the base-station-information recording section 122 constitute a control section 123.

[0034] Hereinbelow, along with the sequence shown in FIG. 1, and also referring to FIGS. 2 to 4, a description will be made regarding operation of the PHS position-information notifying system configured as described above. As described above, two cases can be considered regarding the operation. In one case, a detection request is issued from a client terminal to the position-information converting center 4 to thereby obtain position information. In the other case, the detection-target terminal 1 notifies the position-information converting center 4 of position information at predetermined periods of time. Hereinbelow, the former case will be described with reference to examples.

[0035] First of all, a client terminal performs line connection to the position-information converting center 4 (step S1). Then, the position-information converting center 4 performs the following authentication processing (step S2). Specifically, the position-information converting center 4 determines whether the client terminal to which the line-connection request was issued is a specific registered

terminal determined at the time of conclusion of a position-information service contract (or a backup terminal thereof). If the client terminal is not the registered terminal, the line connection is rejected. If the client terminal is the registered terminal, when the client terminal thereafter logs into the system (step S3), the position-information converting center 4 performs user-authentication processing therefor (step S4). For example, the position-information converting center 4 performs the user-authentication processing by determining whether a pair of a user ID and a password which is transmitted from the client terminal is registered. As a result, if the pair is not registered, the login entry is rejected; and if the pair is registered, the user-authentication processing therefor is completed.

[0036] Upon completion of the line-connection authentication and the user authentication, the client terminal transmits the detection request (step S5), which was issued by the detection-target terminal 1, to the position-information converting center 4 in the same manner as that described for the "step 4" (FIG. 4) in the Related Art. In response to the above, the position-information converting center 4 transmits a calling request of the detection-target terminal 1 to the base station 2 via the network 5 (step S6). According to the above, the base station 2 issues a position-information notification request

to the detection-target terminal 1 (step S7) in the same manner as that described for the "step 2" in the Related Art.

[0037] In the detection-target terminal 1 (portable terminal 100 in FIG. 2), the cryptographic processing section 103 decrypts a radio-wave received via the microantenna 101 and the radio control section 102, and transmits the result to the CS-ID detecting section 104. If a CS-ID is included in the decrypted signal, the CS-ID detecting section 104 detects the CS-ID and transmits it to the control section 106. To achieve the above, the control section 106 is given a function to obtain CS-IDs in units of a period recorded in the position-information-acquisition-period recording section 110. Also, as described above, when a position-information notification request is received from the base station 2, the control section 106 transmits position information including the obtained CS-ID to the cryptographic processing section 103. The cryptographic processing section 103 encrypts the received position information and includes the encrypted position information in a call specification message. The call specification message is then transmitted from the base station 2 to the network 5 via the radio control section 102 and the microantenna 101 (step S8). Thereby, the network 5 transmits the call specification message including the position information to the position-information converting

center 4. At this stage, the following processing is performed in the position-information converting center 4 (position-information converting center 115 in FIG. 3). When the encrypted CS-ID is transmitted from the network 5 (that is, the ISDN 116) to the cryptographic processing section 117 via the circuit interface section 118, the cryptographic processing section 117 transmits the CS-ID, which can be obtained through decryption, to the position-information converting section 121. The position-information converting section 121 referentially accesses the conversion table stored in the base-station-information recording section 122. It thereby obtains latitude/longitude information corresponding to the received CS-ID from the base-station-information recording section 122 (step S9).

[0038] Subsequently, ISDN-line-exchanging steps are performed between the position-information converting center 4 and the detection-target terminal 1 via the base station 2 and the network 5. A call-specification reception message is transmitted from the position-information converting center 4 to the detection-target terminal 1 (steps S10 and S11). Thereafter, when the position-information converting center 4 transmits a disconnection message to the detection-target terminal 1 (steps S12 and S13), the detection-target terminal 1 that has responded thereto transmits a release

message to the position-information converting center 4 (steps S14 and S15). Then, the network 5 transmits a release-completion message to the detection-target terminal 1 (step S16). Concurrently, the position-information converting center 4 transmits a release-completion message to the network 5 (step S17).

[0039] Subsequently, in the position-information converting center 4 (position-information converting center 115 in FIG. 3), the position-information converting section 121 transmits the latitude/longitude information obtained in step S9 to the circuit interface section 118. Then, the cryptographic processing section 117 adds an ID number and the like of the detection-target terminal 1 to the latitude/longitude information, and then encrypts the information. Subsequently, the cryptographic processing section 117 transmits the encrypted latitude/longitude information including the ID number and the like of the detection-target terminal 1 to the client terminal (equivalent to the position-detecting client 3), which was authenticated in steps S2 and S4, via the ISDN 116 (network 5)(step S18). Then, the client terminal decrypts the received encrypted information, and performs processing of, for example, displaying the position of the detection-target terminal 1, based on the latitude/longitude information obtained through the encryption.

[0040] As above, paying attention to the security of the PHS service, description has been made regarding the PHS position-information notifying system of the present embodiment. According to the embodiment, a position-information-service providing company can perform system administration for the specific group of the position-detecting client 3 separately from ordinary services. In addition, encrypting steps and keys can be established in units of the group for which the management is performed. Moreover, in the case where a detection request is issued from a client terminal as the position-detecting client 3 to the position-information converting center 4, communication of encrypted information can be implemented. Since the encryption is provided through restricted services, it can be realized by a restricted low plant/equipment investment. As a result, services in the nature of increased concealment can be provided at a low investment (in other words, with a low financial burden imposed on a user).

[0041] As it is apparent from the configuration shown in FIG. 2, in the embodiment, since the PHS basic function section 107 is provided, no problems occur in call-communication with a specific call-communication destination. Also, a space created by the reduction in the PB keys and the like can instead be used for the battery 111, the power switch 112, and the like. It has already been confirmed

that an advantage can be provided in that a position-information-service terminal having necessary and minimum call-communication functions and high-security characteristics can be fabricated in the size of a business card. In this case, the position-information service was continuously provided for more than 10 days.

[0042]

[Advantages] As described above, according to the present invention, the client terminal that permits detection of a detection-target terminal or acquisition of position information thereof is restricted to the predetermined terminal, thereby allowing the realization of functions that provide high security for the position-information service. Therefore, the behavior of a VIP (very important person) and the location of valuables can be monitored without being known to malicious third parties. According to the invention as described in Claim 2, the client terminal is restricted to at most two terminals including a backup terminal. Therefore, the system can maintain maximum security, and concurrently, can be of service even in an unexpected state where, for example, a malfunction occurs. According to the invention as described in Claim 3, as a terminal configuration, a call-communication destination for detection-target terminals is limited to that set to a predetermined single number. Therefore, significant

advantages can be obtained in that the system cost can be reduced, and the financial burden imposed on a user can be reduced.

[0043] According to the invention as described in Claim 4, since the position-information converting center is connected by cable to the client terminal, investigation for wire-tapping can be easily performed. According to the invention as described in Claim 5, encryption and decryption are performed for information communicated between the detection-target terminal and the PHS radio base station or the position-information converting center, by using common-key cryptograms or public-key cryptograms transmitted using public keys. This enables configuration of the system having favorable characteristics in security and robustness. According to the invention as described in Claim 6, the position-information converting center encrypts latitude/longitude information converted from information specifying the PHS radio base station, and then transmits the encrypted information to the client terminal. Therefore, according to the invention as described in Claim 5 or Claim 6, even when malicious third parties attempt to illegally access the system, their attempts can be rejected.

[Brief Description of the Drawings]

[FIG. 1] FIG. 1 is an explanatory view showing an example PHS-service control sequence executed with a PHS position-

information notifying system according to an embodiment of the present invention.

[FIG. 2] FIG. 2 is a block diagram showing an example configuration of a portable terminal in the system.

[FIG. 3] FIG. 3 is a block diagram showing an example configuration of a position-information converting center in the system.

[FIG. 4] FIG. 4 is a block diagram showing an example configuration of a system for realizing a terminal-position inquiry system by using a conventional technology.

[FIG. 5] FIG. 5 is an explanatory view showing an image of a PHS-used position-information service.

[FIG. 6] FIG. 6 is an explanatory view showing an example PHS-service control sequence executed with a PHS position-information notifying system according to the conventional technology.

[Reference Numerals]

1, 1a, 1b: detection-target terminal; 2, 21-23: base station; 3: position-detecting client; 4: position-information converting center; 5: network; 6: CS interface section; 7: control system; 100: portable terminal; 101: detection-target terminal microantenna; 102: radio control section; 103: cryptographic processing section 103; 104: CS-ID detecting section; 105: signal-level detecting section; 106: control section; 107: PHS basic function section 107;

108: notified-information recording section; 109: notification-period/notification-time recording section; 110: position-information-acquisition-period recording section; 111: battery; 112: power switch; 115: position-information converting center; 116: ISDN; 117: cryptographic processing section; 118: circuit interface section; 120: radio section; 121: position-information converting section; 122: base-station-information recording section; 123: control section; C1-C4, Cx, Cy: cell

Translation of figure:

Translation goes from top to down, from left to right

[FIG. 1]

POSITION-INFORMATION NOTIFYING TERMINAL (DETECTION-TARGET TERMINAL 1)

S7: REQUEST FOR POSITION-INFORMATION NOTIFICATION

S8: ESTABLISH CALL (INCLUDING ENCRYPTED POSITION INFORMATION)

S11: RECEIVE CALL SPECIFICATION

S13: DISCONNECT

S14: RELEASE

S16: COMPLETE RELEASE

NETWORK 5

S6: CALL TERMINAL

S9: ESTABLISH CALL (INCLUDING POSITION INFORMATION)

S10: RECEIVE CALL SPECIFICATION

S12: DISCONNECT

S15: RELEASE

S17: COMPLETE RELEASE

POSITION-INFORMATION CONVERTING CENTER 4

S2: AUTHENTICATE LINE CONNECTION

S4: AUTHENTICATE USER

SERVICE-CONTRACTING REGISTERED TERMINAL

S1: CONNECT LINE

S3: LOG IN

S5: REQUEST FOR DETECTION

S18: NOTIFY ENCRYPTED LATITUDE/LONGITUDE INFORMATION OF DETECTION-TARGET TERMINAL POSITION AND TELEPHONE NUMBER

[FIG. 2]

102: RADIO CONTROL SECTION

103: CRYPTOGRAPHIC PROCESSING SECTION

104: CS-ID DETECTING SECTION

105: SIGNAL-LEVEL DETECTING SECTION

120: RADIO SECTION

112: POWER SWITCH

106: CONTROL SECTION

107: PHS BASIC FUNCTION SECTION

111: BATTERY

108: NOTIFIED-INFORMATION RECORDING SECTION

109: NOTIFICATION-PERIOD/NOTIFICATION-TIME RECORDING SECTION

110: POSITION-INFORMATION-ACQUISITION-PERIOD RECORDING SECTION

[FIG. 3]

122: BASE-STATION-INFORMATION RECORDING SECTION

121: POSITION-INFORMATION CONVERTING SECTION

123: CONTROL SECTION

117: CRYPTOGRAPHIC PROCESSING SECTION

118: CIRCUIT INTERFACE SECTION

[FIG. 4]

2) INFORMATION-NOTIFICATION REQUEST

DETECTION-TARGET TERMINAL

3) BASE-STATION ID NOTIFICATION

5: NETWORK

4: POSITION-INFORMATION CONVERTING CENTER

1: DETECTION REQUEST

4) LATITUDE/LONGITUDE INFORMATION NOTIFICATION

3: POSITION-DETECTING CLIENT

5) MAP DISPLAY

[FIG. 5]

EXAMPLES

BASE-STATION ANTENNA

TELEPHONE BOOTH

CELL SERVICE AREA

6: CS INTERFACE SECTION

ISDN AND CONTROL SYSTEM

[FIG. 6]

[FIG. 1]

POSITION-INFORMATION NOTIFYING TERMINAL (DETECTION-TARGET TERMINAL 1)

REQUEST FOR POSITION-INFORMATION NOTIFICATION

ESTABLISH CALL (INCLUDING POSITION INFORMATION)

RECEIVE CALL SPECIFICATION

DISCONNECT

RELEASE

COMPLETE RELEASE

NETWORK 5

CALL TERMINAL

ESTABLISH CALL (INCLUDING POSITION INFORMATION)

RECEIVE CALL SPECIFICATION

DISCONNECT

RELEASE

COMPLETE RELEASE

POSITION-INFORMATION CONVERTING CENTER 4

AUTHENTICATE LINE CONNECTION

AUTHENTICATE USER

SERVICE-CONTRACTING REGISTERED TERMINAL

CONNECT LINE

LOG IN

REQUEST FOR DETECTION

NOTIFY LATITUDE/LONGITUDE INFORMATION OF DETECTION-TARGET TERMINAL POSITION AND TELEPHONE NUMBER

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－4482
（Ｐ2000－4482Ａ）
(43)公開日　平成12年１月７日(2000.1.7)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｊ０６２
Ｇ０１Ｓ　5/02		Ｇ０１Ｓ　5/02	Ｚ	５Ｋ０６７
Ｈ０４Ｑ　7/34		Ｈ０４Ｂ　7/26	１０６Ａ	

審査請求　未請求　請求項の数６　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－170366

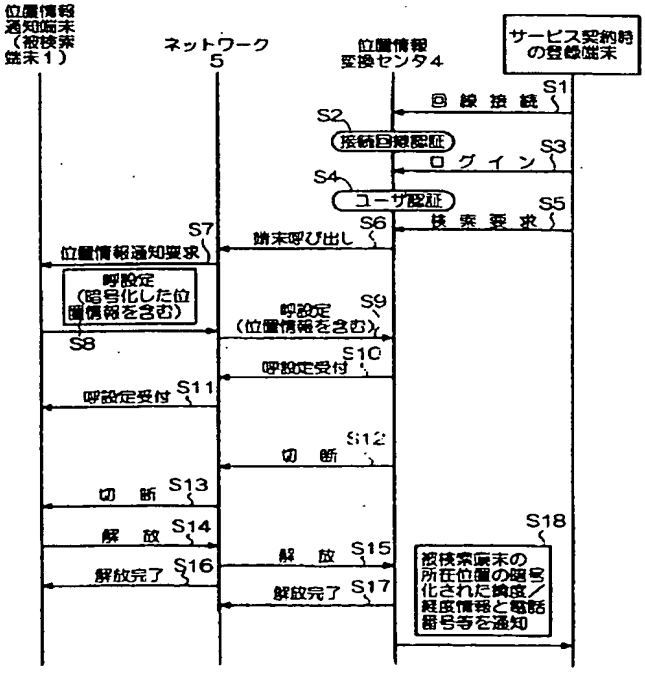
(22)出願日　平成10年６月17日(1998.6.17)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　桜井　哲真
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　荻野　輝雄
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】　ＰＨＳ位置情報通知システム

(57)【要約】
【課題】　位置検索クライアント端末と被検索端末の間で不法な位置情報の取得を許さないＰＨＳ位置情報通知システムを提供する。
【解決手段】　位置情報変換センタ４はクライアント端末から回線接続（Ｓ１）があると、これがサービス契約時の登録端末かどうか認証する（Ｓ２）。その後、クライアント端末からのログイン（Ｓ３）に対してユーザ認証（Ｓ４）を行うとともに、被検索端末１の検索要求（Ｓ５）に対してネットワーク５へ端末呼び出し（Ｓ６）を行い、ネットワーク５から被検索端末１へ位置情報通知要求を行う（Ｓ７）。被検索端末１は暗号化された位置情報を呼設定に含めてネットワーク５から位置情報変換センタ４に送出する（Ｓ８，Ｓ９）。その後、位置情報変換センタ４と被検索端末１の間でＳ１０～Ｓ１７の手順を踏み、位置情報変換センタ４が上記位置情報に対応した緯度／経度情報を暗号化してクライアント端末に送出する（Ｓ１８）。



【特許請求の範囲】

【請求項１】　通信しているＰＨＳ無線基地局を特定する情報を被検索端末が検知して位置情報変換センタに通知し、クライアント端末が前記位置情報変換センタから前記被検索端末の検索あるいは所在の問い合わせを行う通信システムにおいて、

前記位置情報変換センタは、前記被検索端末の検索あるいは所在情報の取得を許す前記クライアント端末を予め決められた特定の端末に限定する認証手段を有することを特徴とするＰＨＳ位置情報通知システム。

【請求項２】　前記認証手段は、前記クライアント端末をバックアップを含めた高々２台の端末に限定することを特徴とする請求項１記載のＰＨＳ位置情報通知システム。

【請求項３】　前記被検索端末の通話用発信先があらかじめ定められた一番号のみに制限されていることを特徴とする請求項１又は２記載のＰＨＳ位置情報通知システム。

【請求項４】　前記位置情報変換センタと前記クライアント端末の間が有線接続されていることを特徴とする請求項１～３の何れかの項記載のＰＨＳ位置情報通知システム。

【請求項５】　前記被検索端末は、前記ＰＨＳ無線基地局又は前記位置情報変換センタとの間で送受信される情報を公開鍵暗号又は公開鍵により送信された共通鍵暗号を用いて暗号化／復号化する手段を有することを特徴とする請求項１～４の何れかの項記載のＰＨＳ位置情報通知システム。

【請求項６】　前記位置情報変換センタは、

前記ＰＨＳ無線基地局を特定する情報を受信して対応する緯度／経度情報に変換する変換手段と、

前記変換手段で変換された前記緯度／経度情報を少なくとも含む情報を暗号化して前記クライアント端末に送出する手段とを有することを特徴とする請求項１～５の何れかの項記載のＰＨＳ位置情報通知システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＰＨＳ（パーソナル・ハンディフォン・システム）無線通信を利用した携帯型の通信機器（被検索端末）の存在場所に対応する情報（以後、「位置情報」と呼ぶ）を緯度／経度情報に変換して端末位置監視端末あるいは位置検索クライアント端末に通知するＰＨＳ位置情報通知システムに関するものである。さらに詳しくは、被検索端末を利用して当該被検索端末の位置情報を位置情報変換センタに送出し、位置情報変換センタが送出された位置情報を緯度／経度情報に変換して端末位置監視端末あるいは位置検索クライアント端末に通知を行い、端末位置監視端末あるいは位置検索クライアント端末が被検索端末の位置を地図や住所などと対応させて管理するＰＨＳ位置情報通知システムに関する。

【０００２】

【従来の技術】現在、ＰＨＳ無線通信を利用した通信端末等の通信機器の中には、当該通信機器の所在する位置情報を送信する機器あるいはその所在する位置が問い合わせ対象となる機器（即ち、上述した被検索端末）が存在しており、それらの情報提供をサービスする会社がある。例えば、ＮＴＴ中央パーソナル通信網（株）の“いまどこサービス”がその一例である。これらの被検索端末が位置情報を送信する契機は、監視センタからの指示（位置検索クライアント端末からのユーザ要求に基づくものを含む）によってその都度通知するか、あるいは、あらかじめ被検索端末内に設定された時刻設定あるいは周期設定等で起動される機能に依っている。

【０００３】図４は、上記サービスに用いられる通信端末とサービスの中心となるセンタ装置の関係を模擬的に示したものである。同図において、１は被検索端末であってＰＨＳ電話機あるいは同等の機能を持つ専用カード型端末等が用いられる。この被検索端末１は、ＰＨＳ電話システムのプロトコルに従って、近くの基地局（以下、図示したように「ＣＳ」と略記することがある）２からの周期的なあるいは単発の呼び出しに応じて、被検索端末１が所在する位置で通信可能な基地局を検索し、当該基地局の特定番号（以下、「ＣＳ－ＩＤ」と称する）や基地局の信号レベル等を通知する。これら一連の情報送信はＰＨＳ電話システムで規定された電波を用いるため、被検索端末１から通知されるこれら情報を受信できる基地局は被検索端末１の近傍おおよそ１００～５００ｍ四方に存在する基地局２に限られる。このような基地局の数は数局であっていずれも近接したものに限られる。そして、これらの基地局のＣＳ－ＩＤ及び設置場所に関する情報はシステム内の位置情報変換センタ４で一括管理されているため、被検索端末１のＩＤ番号等とあわせて受信したＣＳ－ＩＤ番号が判明すれば被検索端末１のおおよその位置が特定できることとなる。

【０００４】以上のような手順の他、基地局側の電波発信強度を高くしたＰＨＳ電話システムの運用も行われている。このような場合には、被検索端末が一度の手順で数ヶ所以上の基地局電波を受信することとなり、近くの基地局アンテナを特定することが困難な場合がある。こうした困難を克服するための手段として、受信電波強度に応じた演算を行って位置を検出することも実験的になされている。これは、受信した基地局のＣＳ－ＩＤを緯度／経度情報に読替えると共に、受信電波強度を各受信基地局の“重さ”とし、受信基地局を頂点とする多角形の重心を求めることによって、被検索端末のおおよその位置を求める手順である。この他、受信電波強度がほぼ等しい二つの基地局間を結ぶ線分の垂直二等分線を二組求めて、それらの交点を被検索端末のおおよその位置とする手法等も実験的に利用されている。

【０００５】これらの原理に基づいて被検索端末の位置を実用的なレベルで特定することが可能なため、ＰＨＳ電話システムを利用した位置情報サービスが平成１０年春より開始されている。例えば、親が子供の遅い帰りを心配して位置情報を問い合わせたり、あるいは、修学旅行等の自由行動で学生のグループの行動を同行せずに把握したりするなどの具体的な利用が始まっている。

【０００６】なお、図４において、位置検索クライアント３はパーソナルコンピュータ（以下、「パソコン」という）やワークステーションの如きものでもよいが、これらに加えて、検索すべき被検索端末を特定する情報が発信できるものなら何を用いてもよい。例えば、一般の電話やＦＡＸ（ファクシミリ）端末等の利用も可能であり、平成９年秋から山形県酒田市で行われた徘徊老人の為の位置検索サービスでは、パソコンに加えてＦＡＸ及び一般の電話も利用されていた。ちなみに、このケースでは、ＦＡＸや電話から被検索端末を特定する方法は当該被検索端末の番号をＦＡＸや電話のプッシュボタンで入力することであった。また、図４に示したネットワーク５としてはＩＳＤＮ（サービス総合ディジタル網）等を用いる。

【０００７】ここで、現在提供されている位置情報サービスの手順を具体的に説明する。図４に示す模式的なシステム構成及びサービスにおいて、まず、被検索端末１の位置情報の検索要求が、位置検索クライアント３からネットワーク５を経由して位置情報変換センタ４に上げられる（手順１）。これを受けて、位置情報変換センタ４はネットワーク５および基地局２を経由して当該被検索端末１へ情報通知要求を行う（手順２）。被検索端末１は、自己が所在する位置で受信可能な基地局２を検索して、当該基地局のＣＳ－ＩＤをネットワーク５を経由させて位置情報変換センタ４に送り返す（手順３）。位置情報変換センタ４は受信した基地局のＣＳ－ＩＤと対応づけた所在位置情報（緯度及び経度）を事前にテーブル形式で保有しているので、送られてきたＣＳ－ＩＤを直ちに緯度／経度情報に読み替える（手順４）。次いで、位置情報変換センタ４はこの緯度／経度情報をネットワーク５を経由して位置検索クライアント３に届ける。これにより、位置検索クライアント３は、別に保管している地図情報と重ね合わせて被検索端末１の位置のＣＲＴ（陰極線管）表示を行うことが可能になる（手順５）。

【０００８】なお、位置検索クライアント３にＦＡＸを用いた場合には、位置情報変換センタ４からＦＡＸ信号で位置検索クライアント３に通知することによって、ＦＡＸ画像として表示することが可能となる。また、位置検索クライアント３に電話機などを使用した場合、位置情報変換センタ４は所在位置の情報を音声に変換（一例として「指定の端末は＊＊市＃＃区@@町＄＄番地にいます」に変換する）して、電話機から音声による出力を行うことが可能である。

【０００９】それでは次に、ユーザが移動した時の位置情報の取得につき図５を用いて具体的に説明する。なお、図５における各部の形状は分かり易さを優先して表現してあり、また、図４に示したものと同じ構成要素には同一の符号を付してある。図５において、基地局２１，２２，２３等は図４に示した基地局２と同等の基地局であって、符号６，６，…，６はこれらの基地局をそれぞれ管理するＣＳインタフェース部である。また、ＩＳＤＮ及び制御システム７は図４に示したネットワーク５に相当しておりＣＳインタフェース部６，６，…，６が接続されている。以上に加えて、ユーザの所持する被検索端末１（なお、移動した被検索端末１を符号１ａ，１ｂ等と表記してある）や被検索端末１以外の図示しない複数の端末等によってＰＨＳ電話システムが構成されており、かかるＰＨＳ電話システムは以下に述べるＰＨＳ電話サービスを提供する。

【００１０】また、こうしたＰＨＳ電話システムでは、ＰＨＳ相互の通信サービスだけでなく、図示しない他のネットワーク（例えばＰＳＴＮ（公衆電話交換網）あるいはインターネット等）とつながっているか或いはつなげることも可能であって、さらには、一般の家庭電話などとの通話も可能である。これらに加えて、本発明の適用領域である位置情報サービスが、昨今、ＰＨＳ電話システムに加えられた。なお、以下の記述では、電話以外のサービスあるいはシステムも含むことから、先のＰＨＳ電話サービスの表記に代えて「ＰＨＳサービス」と表記するとともに、ＰＨＳ電話システムの表記に代えて「ＰＨＳシステム」と表記する。

【００１１】以上のように多彩なサービスが可能なＰＨＳサービスは、１．９ＧＨｚ帯の電波を用い、携帯端末からは１０ｍＷ以下の無線（以下、「ＲＦ」と表記）出力，公衆基地局側（即ち、基地局２１，２２，２３等）からは５００ｍＷ以下の出力（意図する基地局のカバー範囲によって出力値を制御可能）で、１スロットあたり３２ｋｂｉｔ／ｓ迄の音声あるいはディジタルデータの送受信を行うパーソナルユースの通信サービスである。また、ＰＨＳシステムにおいては、ＴＤＭＡ／ＴＤＤ（時分割多元接続／時分割二重）フレームと呼ばれる５ｍｓ毎の単位時間の中で送受信のタイムスロット（６２５μｓ／スロット）が割り当てられ、一つの基地局に対して三つの端末の音声チャネルが設けられる。また、この音声チャネルを制御するためのチャネルたる「制御チャネル」が一つの基地局と三つの端末の間に設けられている。当然のことであるが、これらの数値は現状のものであり、今後、社会的要請あるいは技術的進歩でこれらの数値が変わることもあり得る。その場合にも本発明の主旨が損なわれないことは明らかである。

【００１２】電話としてのＰＨＳサービスは端末の低速移動（おおむね３０ｋｍ／時以下であるが、セルの大き

さに依存するために、ＰＨＳサービスを提供する会社毎に若干の大小が存在する。以下、「ＰＨＳの許容所定速度」と表記）を許容しており、常にユーザの端末の位置をシステム側で記憶している必要がある。そこでこの仕組について図５を参照して簡単に述べる。いま、基地局２１，２２，２３が発する電波の受信可能範囲をそれぞれ、セルＣ１，セルＣ２，セルＣ３とし、また、図示しない基地局が発する電波の受信可能範囲をセルＣ４，Ｃｘ，Ｃｙ等とする。また、被検索端末１は最初はセルＣ１内に居て、その後、セルＣ２，セルＣ３へと順次移動する（前述したように図５では被検索端末１ａ，１ｂとして表示）ものと仮定する。また、前述したように被検索端末１とは別に図示しない被検索端末が複数存在するものとする。

【００１３】これら数多い端末の位置を特定して記録する作業（以下、「位置登録」と呼ぶ）に対して、端末の移動の度に利用可能な基地局の登録を行うことは電波の輻輳を招くので“一斉呼び出し”と呼ばれる手順を踏む。ここで言う一斉呼び出しとは、複数の公衆基地局を取りまとめて位置登録エリア（例えば、セルＣ１とセルＣ２で一つの位置登録エリアを形成する）とし、被検索端末１等のＰＨＳ端末は、公衆基地局毎にではなく位置登録エリアが変わった時のみ位置登録を行うとともに、着信を行う場合にはＰＨＳ端末が存在する可能性のある位置登録エリア内の複数の公衆基地局のそれぞれがＰＨＳ端末に呼び出しを行い、ＰＨＳ端末から応答のあった公衆基地局のみが当該ＰＨＳ端末に対して着信を行うというものである。

【００１４】

【発明が解決しようとする課題】以上の手順において、不法な電波傍受による位置情報の横取りを避ける手立てが講じられている。例えば、公衆基地局とＰＨＳ端末の間の情報授受に際しては、秘匿鍵設定／認証要求／認証応答といった通常の暗号化通信が採られており、電波傍受による位置情報の横取りはかなり困難な状況にあるといえる。また、図４に示す位置検索クライアント３（あるいは同等の機能を果たす電話機あるいはＦＡＸ端末）から位置情報変換センタ４への位置検索要求の発信（発呼）に際しては、認証要求／認証番号入力／暗証（パスワードとも称する）番号要求／暗証番号入力と言った一連の手順が尽くされており、秘匿性（以下、「セキュリティ」と称する）を高めているとされてきた。

【００１５】このようなセキュリティへの配慮にもかかわらず、システム全体の頑健性は改善すべき余地がある。その最たる部分はユーザとのインタフェースである。ここで、図６に一般的なＰＨＳサービスの手順を示す。図示したように、位置検索クライアント３等の端末（図中の“端末位置監視センタ又は要求端末”）から位置情報変換センタ４へのアクセスは二段構えで防御されている。その一つがアクセスする回線の認証（図中の“接続回線認証”）であり、他の一つはアクセスするユーザの認証（図中の“ユーザ認証”）である。

【００１６】しかし、回線の認証に際しては、位置情報変換センタ４にアクセス可能な不正取得された携帯端末によってセキュリティが破られる可能性がある。また、ユーザ認証に際してはパスワードでのガードが存在するものの、悪意のある第三者が位置情報の検索要求に必要な暗証を入手することが現実として考え得る。これは、位置情報検索サービスのパスワードはユーザ自身が覚えている必要があるが、入力の際の間違いを防ぐためにパスワードとして簡単な英字列や数字列が選ばれることが多いことに起因している。例えば、数字列のパスワードの代表事例が銀行のキャッシュカードである。誕生日や自宅の郵便番号等の推定し易いものを用い勝ちなこの種のパスワードが簡単に破られるのは、不正に取得したキャッシュカードによる現金引き出しが多発していることからも明らかである。このようなことからも明らかなように、プライバシーが守られるべき個人情報あるいは貴重な事物の所在を悪意の第三者が比較的簡単に知り得る可能性がある。

【００１７】本発明は上記の点に鑑みてなされたものであり、その目的は、被検索端末がＰＨＳ無線基地局を特定する情報及び受信信号レベルを検知してこれらの情報を位置情報変換センタから位置検索クライアント端末等に通知する通信システムにおいて、位置情報が通知される端末と被検索端末との間でセキュリティに関する密接な関係を設けて、悪意の第三者による不法な位置情報の取得を許さないＰＨＳ位置情報通知システムを提供することにある。

【００１８】

【課題を解決するための手段】以上の課題を解決するために、請求項１記載の発明は、通信しているＰＨＳ無線基地局を特定する情報を被検索端末が検知して位置情報変換センタに通知し、クライアント端末が前記位置情報変換センタから前記被検索端末の検索あるいは所在の問い合わせを行う通信システムにおいて、前記位置情報変換センタは、前記被検索端末の検索あるいは所在情報の取得を許す前記クライアント端末を予め決められた特定の端末に限定する認証手段を有することを特徴としている。また、請求項２記載の発明は、請求項１記載の発明において、前記認証手段は、前記クライアント端末をバックアップを含めた高々２台の端末に限定することを特徴としている。また、請求項３記載の発明は、請求項１又は２記載の発明において、前記被検索端末の通話用発信先があらかじめ定められた一番号のみに制限されていることを特徴としている。すなわち、被検索端末の通話用発信先はクライアント端末と密接に関係するあらかじめ定められた一番号に制限されるものであって、この一番号としては、クライアント端末の置かれた室の電話の番号、あるいは、被検索端末を管理する人物につながる

番号を選ぶ。

【００１９】また、請求項４記載の発明は、請求項１～３の何れかの項記載の発明において、前記位置情報変換センタと前記クライアント端末の間が有線接続されていることを特徴としている。また、請求項５記載の発明は、請求項１～４の何れかの項記載の発明において、前記被検索端末は、前記ＰＨＳ無線基地局又は前記位置情報変換センタとの間で送受信される情報を公開鍵暗号又は公開鍵により送信された共通鍵暗号を用いて暗号化／復号化する手段を有することを特徴としている。また、請求項６記載の発明は、請求項１～５の何れかの項記載の発明において、前記位置情報変換センタは、前記ＰＨＳ無線基地局を特定する情報を受信して対応する緯度／経度情報に変換する変換手段と、前記変換手段で変換された前記緯度／経度情報を少なくとも含む情報を暗号化して前記クライアント端末に送出する手段とを有することを特徴としている。

【００２０】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態について説明するが、最初に本発明の概要を説明しておく。本発明は、位置情報の問い合わせ対象となる端末機器である被検索端末と当該問い合わせを行う端末位置監視端末あるいは位置検索クライアント端末の両者を組にして、組外からの問い合わせ行為を認めないＰＨＳ位置情報通知システムである。そのために本発明では、被検索端末と位置検索クライアント端末等との間に特定の相互認証関係を設けて、不正な第三者の介入を許さない仕組を提供している。また本発明では、かかる相互認証に加えて、位置情報を暗号化された形態で送受することにより、仮に不法な手段でアクセスする悪意の第三者が存在してもその目的を達し得ない仕組を提供するものである。

【００２１】さて、図１は本実施形態による位置情報の検索手順の一例を示したものであり、その手順の詳細については後述することとして、ここでは従来との相違点を中心に説明する。先に示した従来の事例（図６参照）と大きく異なる第一の点は、被検索端末１の検索あるいは所在情報の取得を許すクライアント端末を限定することにある。つまり本実施形態では、図４に示した位置検索クライアント３を位置情報サービス契約時に決められた特定の端末（即ち、図１に示す“サービス契約時の登録端末”）だけにしている。ここで、この限定の度合としては、クライアント端末を一台とし且つこのクライアント端末を有線接続されたものとすることが最も好ましい。これは有線接続されたものが盗聴されているか否かの調査がし易いことによる。なお、故障等の不測の事態に備えてバックアップのクライアント端末を一台用意することが現実的である。このような形態に加えて、被検索端末から特定の一番号への発信を可能とするようにしても良い。この一番号としては、被検索端末所持者からクライアント端末操作者あるいは被検索端末の管理者へつながる番号とする。こうして一台の端末が被検索端末からの着信番号を持つこととなる。

【００２２】ここで、図４に示した被検索端末１以外にも複数の端末がシステムに存在することがあるが、こうした形態はもちろん本発明の範囲内である。また、バックアップを含む高々二台のクライアント端末と複数の被検索端末の組からなるグループが一つのＰＨＳサービスシステムに複数組存在することもあるが、こうした形態も本発明の範囲内である。但し、この場合でも別のグループに属するクライアントがそのクライアントの属するグループ以外の端末の検索を行うことは本発明の趣旨を逸脱するものであり、そのような行為を防ぐためのシステム的なセキュリティが存在している。具体的には、クライアント端末からの検索要求に対して、〔発明が解決しようとする課題〕の冒頭に示した一連の手順を尽くすことである。

【００２３】このように位置情報の取得あるいは検索要求が出せるクライアント端末を限定すると、従来のように正確なパスワードを提示しさえすればどのような端末からでも位置情報サービスの利用が可能なサービスに比べて、サービスの質の低下があるようにも見える。しかしながら、熟慮すれば明らかなように、時々刻々変化する位置情報を統制管理すべきクライアント端末を限定された人に割り当て、或いは限定された場所に設置して、その連絡番号（即ち、連絡電話番号，ＦＡＸ番号，メールアドレスあるいはＵＲＬ（Uniform Resource Locator）等の端末識別番号）も限られたものにすることで、非常時の迷いがなくなって好ましいことは明らかである。

【００２４】これに加えて、ＰＨＳサービスにあるように特定の番号のみに発信する電話では、ＰＢ（プッシュボタン）機能等を不要とすることができ、被検索端末自身の軽量化及び低コスト化，被検索端末１を所持するユーザの操作の手間の軽減，（特定の端末にしか着信できないことにより）被検索端末を不正に取得した悪意の第三者による無法な乱用の防止等、現行の電話機あるいはＰＨＳ端末に無い大きな利点を獲得することは明白である。事実、発明者らは電源ボタンの押すパターンを特定の押し方とすることで、実験システムの指定した番号への着信を実現している。もっとも実際のサービスにおいては、電源の切断あるいは投入のための操作を特殊な電源ボタン操作として、特定番号への着信あるいは応答を電源ボタンを一押しする操作で可能とすることの方が現実的ではある。

【００２５】一方、本実施形態の第二の特徴は、位置情報変換センタ４からサービス契約時の登録端末への情報（即ち、被検索端末１が所在する位置の緯度／経度情報及び被検索端末１のＩＤ番号ないし電話番号等）を暗号化していることである。昨今、暗号化のアルゴリズムや

システムは種々のものが提案／実用化されており、代表的なものとしては、共通鍵暗号と呼ばれる処理速度重視のＦＥＡＬ（高速暗号化アルゴリズム）－８やＲＣ５のほか、処理速度に制限があるものの安全性の大きなＭＩＳＴＹあるいはＳＱＵＡＲＥなどの公開鍵暗号が挙げられる。ただ、このような暗号を利用した場合には安全性（頑健性）と遅延の少ない情報伝送の両立は困難である。

【００２６】しかしながら、本実施形態における暗号化の適用領域は“被検索端末の所在位置の緯度／経度情報及び被検索端末のＩＤ番号”という極めて限定されたものであって、短い数字列あるいは英文字列で表現することができる。それゆえ本実施形態では、長い文字列の変換には向かないが頑健性は高いとされている公開鍵暗号方式を採用することが可能である。即ち、本実施形態の適用対象である位置検索クライアント３は、位置情報変換センタ４との間で公開鍵暗号方式の暗号化鍵と復号鍵をそれぞれ持っており、それによって相手のみに向けた守秘性の高い通信を容易に行うことが可能である。またこの応用として、公開鍵暗号によって共通暗号の鍵を送り、長い文字列あるいは長い通信を現実的な処理時間で行う方式も取り得る。このような仕組みは、先に指摘した有線接続による通信の盗聴を無駄なものとするという大きな効果をもたらす。当然であるが、位置情報変換センタ４そのものに悪意の第三者が侵入すると全ての努力が水泡に帰すため、位置情報変換センタ４をイントラネットの防護内に配置することは極めて重要である。

【００２７】次に、図２は本実施形態における携帯端末の具体的な構成例を模式的に示したものであって、図示した携帯端末１００は以下の構成を有している。まず、超小形アンテナ１０１はＰＨＳ規格の電波を送受するインタフェースであって、セラミックアンテナチップ等で構成されている。無線部１２０は、超小形アンテナ１０１で送受されるＰＨＳ規格の電波を処理するものであって、無線制御部１０２，暗号処理部１０３，ＣＳ－ＩＤ検出部１０４，信号レベル検出部１０５を有する。無線制御部１０２は超小形アンテナ１０１を介したＰＨＳ規格の電波の送受信を司っている。暗号処理部１０３は、無線制御部１０２が受信したＰＨＳ規格の電波に含まれる信号が暗号化された信号である場合に当該信号を復号化するほか、制御部１０６の指示に従って制御部１０６から送られてくる情報を暗号化し無線制御部１０２を介して超小形アンテナ１０１から送信する。ＣＳ－ＩＤ検出部１０４は暗号化処理部１０３で復号化された信号からＣＳ－ＩＤを検出して制御部１０６（後述）に送出する。こうしてＣＳ－ＩＤが明らかにされることで、必要な処理手順が制御部１０６の管理の下に尽くされる。一方、信号レベル検出部１０５はＰＨＳ規格の電波の電波強度を分析し、無線制御部１０２に対して最適な受信のためのいわゆるチューニングを施す。

【００２８】次に、制御部１０６はエネルギー消費までも含む携帯端末１００内の全体制御を担っており、また、ＰＨＳ基本機能部１０７は主に通話の制御を行っている。このように、制御部１０６の制御機能とＰＨＳ基本機能部１０７はモジュール（機能）として独立していることが望ましい。これは、携帯端末１００全体のエネルギー消費までも含む制御とＰＨＳシステムを用いた通話サービス機能の制御とでは異なることが多いためである。そして、前者にはいわゆるＲＩＳＣ（縮小命令セットコンピュータ）チップを用い、後者にはＤＳＰ（ディジタル信号処理プロセッサ）チップを用いることが効果的である。ただ、昨今、システムＬＳＩ（大規模集積回路）の概念の下に両者の機能を合わせ持つものも出現しているので、いま述べたことは必須な条件というわけではない。当然であるが、ＰＨＳ基本機能部１０７が主に通話の制御を行う一方で、本発明の適用領域である位置情報サービスあるいは位置検索サービスに適した制御部１０６等のモジュールを内蔵させることがシステムの実用性を高めている。

【００２９】以上に加えて、発明者らの先行実験により位置情報の通知履歴を管理することが最も重要であることがわかったので、本実施形態ではそれに対応したモジュールを内蔵している。すなわち、今までに通知した情報を一元管理する既通知情報記録部１０８，位置情報を通知すべき周期ないし時刻が格納された通知周期／通知時刻記録部１０９，公衆無線局から送られるＣＳ－ＩＤ等の位置情報を取得する周期が格納された位置情報取得周期記録部１１０がこれに相当する。そして制御部１０７は、既通知情報記録部１０８に蓄積されている位置情報の通知履歴と新たに受信したＣＳ－ＩＤの情報とを比較して、ＣＳ－ＩＤの変化を検知したときに位置情報の通知処理を行う。また、検索されたＣＳ－ＩＤが１種類の場合には、基地局のサービスエリア端近傍やビル内などの電波が届きにくい場所に移動しつつあり、そのまま放置すると次の位置情報通知を契機として電波状況が著しく悪化して通知不可となる可能性があるが、こうした事態に至る前に制御部１０７はその状況を基地局等に通知することなども可能となる。

【００３０】以上のように、既通知情報記録部１０８，通知周期／通知時刻記録部１０９及び位置情報取得周期記録部１１０は、本携帯端末１００の操作が困難な徘徊老人等のユーザが操作上の負担を負うことなくＰＨＳの位置情報サービスを享受するためのものである。そして、これらに記録されたタイミングで位置情報が自動的にネットワーク５を経由して位置情報変換センタ４に向けて発信される。一方、図２において符号１１１は携帯端末１００の各部に電源を供給する電池であり、符号１１２は前述した電源ボタンなどから構成される電源スイッチである。

【００３１】次に、図３に基づいて本実施形態による位

置情報変換センタ（図４参照）の具体的な構成例について説明する。同図に示すように、本実施形態による位置情報変換センタ１１５は、ＰＨＳサービスのインフラストラクチャであるＩＳＤＮ１１６（図４のネットワーク５に相当）を介し、図４の基地局２（あるいは図５の基地局２１，２２，２３等）や位置検索クライアント３との間で情報の送受信を行う。ここで、ＩＳＤＮ１１６を介して基地局から送信されてくるＣＳ－ＩＤはそのままでは位置情報のサービスに供することができないことから、以下に説明する各部の働きにより、送信されてくるＣＳ－ＩＤを当該ＣＳ－ＩＤに対応する緯度／経度情報に変換している。

【００３２】回線インタフェース部１１８はＩＳＤＮ１１６との間の送受信を司るインタフェースであって、本実施形態ではこの回線インタフェース部１１８が重要な役割を担っていることに注意する必要がある。すなわち、ＩＳＤＮネットワークは暗号化された信号の送受を前提にしていないために、通話先あるいは通話元を特定する電話番号等の基本情報を暗号化することができない。そこで回線インタフェース部１１８は、最初の手順である通話先／通話元の特定が済んでいわゆる電話回線がつながるまでは通常の回線インタフェースとして機能し、通話相手との間で情報の送受が開始される直前に処理を暗号処理部１１７に委ねるようにしている。なお、一般的な通話のみの場合には、暗号化処理を暗号処理部１１７ではなくＰＨＳサービスのスクランブル処理に委ねることも現実的な選択である。

【００３３】暗号処理部１１７は、ＩＳＤＮ１１６を介して基地局から送られるＣＳ－ＩＤを検出して、当該ＣＳ－ＩＤが暗号化されている場合にはそれを復号化して位置情報変換部１２１に渡す。位置情報変換部１２１は、基地局情報記録部１２２が内蔵している変換テーブル（即ち、基地局情報であるＣＳ－ＩＤと対応する緯度／経度情報を読み替えるためのファイルないし記録）を元にして、暗号処理部１１７から渡されたＣＳ－ＩＤを当該ＣＳ－ＩＤの緯度／経度情報に読み替え、得られた緯度／経度情報を表す英数字列を回線インタフェース部１１８に送出する。上述の暗号処理部１１７は回線インタフェース部１１８を介して送られる緯度／経度情報に被検索端末１のＩＤ番号等を付加したのちに、これら情報を暗号化してＩＳＤＮ１１６から位置検索クライアント３に送出する。なお、図示したように、位置情報変換部１２１及び基地局情報記録部１２２は制御部１２３を構成している。

【００３４】次に、図１に示した動作シーケンスに沿って図２～図４等も参照しながら、上記構成によるＰＨＳ位置情報通知システムの動作について説明する。なお、上述したように、クライアント端末から位置情報変換センタ４へ検索要求を行って位置情報を取得する場合と、被検索端末１があらかじめ設定された時刻あるいは周期で位置情報検索センタ４に対して位置情報を通知する場合が考えられるが、ここでは前者の場合を例に挙げて説明することにする。

【００３５】まず、或るクライアント端末が位置情報変換センタ４に対して回線接続を行う（ステップＳ１）と、位置情報変換センタ４は次に述べるような接続回線の認証を行う（ステップＳ２）。すなわち位置情報変換センタ４は、回線接続要求のあったクライアント端末が位置情報サービス契約時に決められた特定の登録端末（もしくはそのバックアップ端末）であるかどうかを判別し、もし当該クライアント端末が登録端末でない場合には回線接続を拒否する。これに対して、当該クライアント端末が登録端末であるならば、位置情報変換センタ４はその後にクライアント端末がログイン（ステップＳ３）してきた場合にそのユーザ認証を行う（ステップＳ４）。例えば、位置情報変換センタ４はクライアント端末から送られてくるユーザＩＤとパスワードの組が予め登録されているかどうかによってこのユーザ認証処理を行うようにして、これらの組が登録されていない場合にはクライアント端末からのログインを拒否する一方で、これらの組が登録されていればユーザ認証処理を完結させる。

【００３６】こうして接続回線認証及びユーザ認証が完了すると、クライアント端末は従来技術の“手順１”（図４）で説明したのと同様にして、位置情報変換センタ４へ被検索端末１の検索要求を送出する（ステップＳ５）。これを受けて位置情報変換センタ４は、ネットワーク５を介して基地局２へ被検索端末１の呼び出し要求を送出する（ステップＳ６）。これにより基地局２は、従来技術の“手順２”で説明したのと同様にして、被検索端末１へ位置情報の通知要求を行う（ステップＳ７）。

【００３７】ここで、被検索端末１（図２の携帯端末１００）では、暗号処理部１０３が超小形アンテナ１０１及び無線制御部１０２を介して受信した電波を復号してＣＳ－ＩＤ検出部１０４に送出する。ＣＳ－ＩＤ検出部１０４は復号化された信号にＣＳ－ＩＤが含まれていれば、当該ＣＳ－ＩＤを検出して制御部１０６に送出する。そこで制御部１０６は位置情報取得記録部１１０に格納されている周期毎にＣＳ－ＩＤを取得するようにする。そして、前述したように基地局２から位置情報通知要求があると、制御部１０６は取得しておいたＣＳ－ＩＤの含まれた位置情報を暗号処理部１０３に送出する。暗号処理部１０３は送られた位置情報を暗号化して呼設定メッセージに含め、当該呼設定メッセージを無線制御部１０２，超小形アンテナ１０１を介して基地局２からネットワーク５に送出する（ステップＳ８）。これにより、ネットワーク５は位置情報変換センタ４に対して位置情報の含まれた呼設定メッセージを送出する。その際、位置情報変換センタ４（図３の位置情報変換センタ

１１５）では以下の処理が行われる。すなわち、ネットワーク５（即ち、ＩＳＤＮ１１６）から回線インタフェース部１１８を介して暗号化されたＣＳ－ＩＤが暗号処理部１１７に送られると、暗号処理部１１７はこれを復号化して得られるＣＳ－ＩＤを位置情報変換部１２１に送出する。位置情報変換部１２１は基地局情報記録部１２２上の変換テーブルを参照して、送られてきたＣＳ－ＩＤに対応する緯度／経度情報を基地局情報記録部１２２から取得する（以上、ステップＳ９）。

【００３８】これ以後は、位置情報変換センタ４と被検索端末１との間で基地局２及びネットワーク５を介してＩＳＤＮの回線交換制御手順が行われる。即ち、位置情報変換センタ４から被検索端末１に対して呼設定受付メッセージが送出（ステップＳ１０，Ｓ１１）され、その後に位置情報変換センタ４が切断メッセージを被検索端末１に送出（ステップＳ１２，Ｓ１３）すると、これに応答した被検索端末１は解放メッセージを位置情報変換センタ４に送出する（ステップＳ１４，Ｓ１５）。これによってネットワーク５が被検索端末１に対して解放完了メッセージを送出する（ステップＳ１６）一方で、位置情報変換センタ４がネットワーク５に対して解放完了メッセージを送出する（ステップＳ１７）。

【００３９】次に、位置情報変換センタ４（図３の位置情報変換センタ１１５）では、位置情報変換部１２１が先のステップＳ９で取得した緯度／経度情報を回線インタフェース部１１８に送出する。すると、暗号処理部１１７は当該緯度／経度情報に被検索端末１のＩＤ番号等を付加してこれらを暗号化したのち、暗号化された緯度／経度情報及び被検索端末１のＩＤ番号等をＩＳＤＮ１１６（ネットワーク５）を経由して、先のステップＳ２，Ｓ４で認証を行ったクライアント端末（位置検索クライアント３に相当）に送出する（ステップＳ１８）。これによりクライアント端末は、送られた暗号化情報を復号化し、この復号化によって得られた緯度／経度情報等に基づいて被検索端末１の位置を地図上に表示させるなどの処理を行う。

【００４０】以上、ＰＨＳサービスのセキュリティ性に着目して本実施形態によるＰＨＳ情報通知システムについて説明した。本実施形態によれば、位置情報サービス提供会社は、特定の位置検索クライアント３のグループを一般のサービスと分離したシステム運営を行うことが可能である。また、こうした管理を行うグループ毎に暗号化の手順と鍵を取り決めることも可能である。さらに、位置検索クライアント３のようなクライアント端末からの検索要求が位置情報変換センタ４になされた場合、暗号化による情報の送受が可能になる。このような暗号化は限定されたサービスであることから限定された設備投資で実現することが可能である。その結果、少ない投資（言葉を替えれば、少ないユーザ負担）で秘匿性を高めたサービスを提供することが可能である。

【００４１】また、本実施形態においては、図２の構成からも明らかなように、ＰＨＳ基本機能部１０７が存在するため、特定の通話先との通話には支障がない。また、ＰＢキー等の削減によってできた容積を電池１１１や電源スイッチ１１２等に余裕として回すことができるので、必要にして最小限の通話機能と高いセキュリティ性を持つ位置情報サービス対応の端末を名刺サイズの大きさの中に収められるという効果も確認できている。この場合の位置情報サービスの連続提供日時は１０日を越える長い期間のものであった。

【００４２】

【発明の効果】以上説明したように、本発明では、被検索端末の検索あるいは所在情報の取得を許すクライアント端末を予め決められた特定の端末に限定することにより、位置情報サービスに対して高いセキュリティをもたらす仕組を実現し得るため、ＶＩＰ(Very Important Person）の行動や貴重な事物の所在を悪意の第三者に知られることなく監視できる。また、請求項２記載の発明では、クライアント端末をバックアップを含めた高々２台の端末に限定しているので、セキュリティを最大限に維持しながら故障等の不測の事態にも対応することができる。また、請求項３記載の発明では、被検索端末の通話用発信先をあらかじめ定められた一番号のみに制限するという端末構成とすることで、システムコストの削減やユーザの負担軽減等をもたらすなど大きな効果がある。

【００４３】また、請求項４記載の発明では、位置情報変換センタとクライアント端末の間を有線接続しているので、盗聴されているか否かの調査が容易になる。また、請求項５記載の発明では、被検索端末がＰＨＳ無線基地局又は位置情報変換センタとの間で送受信される情報を公開鍵暗号又は公開鍵暗号で送信された共通鍵暗号を用いて暗号化／復号化しているので安全性と頑健性を兼ね備えたシステムを構築することができる。また、請求項６記載の発明では、位置情報変換センタがＰＨＳ無線基地局を特定する情報から変換される緯度／経度情報を暗号化してクライアント端末に送出するようにしている。それゆえこれら請求項５又は請求項６記載の発明によれば、仮に不法な手段でアクセスする悪意の第三者が存在してもその目的を阻止することができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態によるＰＨＳ位置情報通知システムで行われるＰＨＳサービスの制御シーケンスの一例を示した説明図である。

【図２】　同システムにおける携帯端末の一構成例を示したブロック図である。

【図３】　同システムにおける位置情報変換センタの一構成例を示したブロック図である。

【図４】　従来の技術を用いて端末位置問い合わせサービスを実現するためのシステムの一構成例を示したブロック図である。

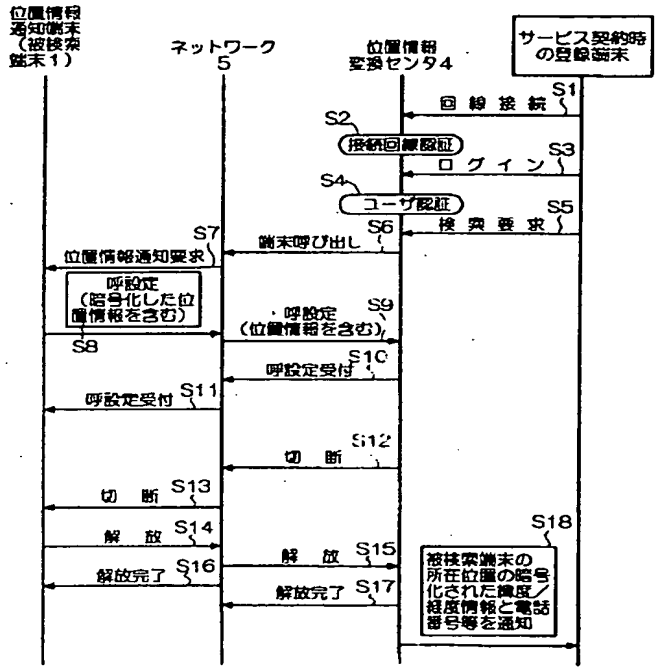
【図５】　ＰＨＳを用いた位置情報サービスのイメージを示した説明図である。

【図６】　従来の技術によるＰＨＳ位置情報通知システムで行われるＰＨＳサービスの制御シーケンスの一例を示した説明図である。

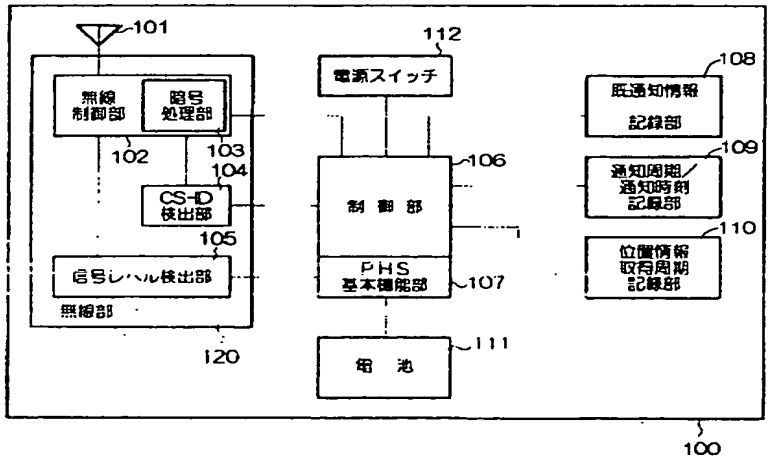
【符号の説明】

１，１ａ，１ｂ…被検索端末、２，２１～２３…基地局、３…位置検索クライアント、４…位置情報変換センタ、５…ネットワーク、６…ＣＳインタフェース部、７…ＩＳＤＮ及び制御システム、１００…携帯端末、１０１…超小形アンテナ、１０２…無線制御部、１０３…暗号処理部、１０４…ＣＳ－ＩＤ検出部、１０５…信号レベル検出部、１０６…制御部、１０７…ＰＨＳ基本機能部、１０８…既通知情報記録部、１０９…通知周期／通知時刻記録部、１１０…位置情報取得周期記録部、１１１…電池、１１２…電源スイッチ、１１５…位置情報変換センタ、１１６…ＩＳＤＮ、１１７…暗号処理部、１１８…回線インタフェース部、１２０…無線部、１２１…位置情報変換部、１２２…基地局情報記録部、１２３…制御部、Ｃ１～Ｃ４，Ｃｘ，Ｃｙ…セル

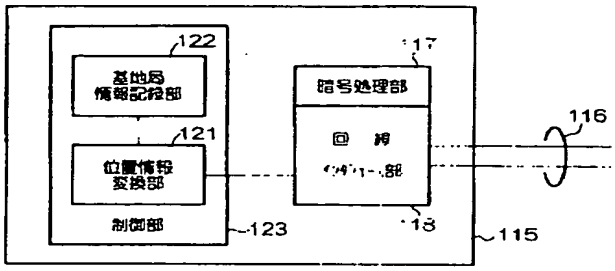
【図１】



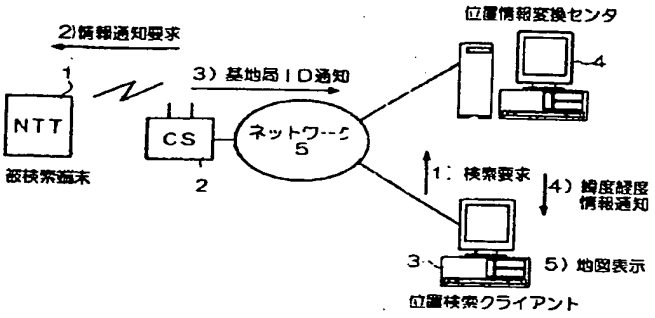
【図２】



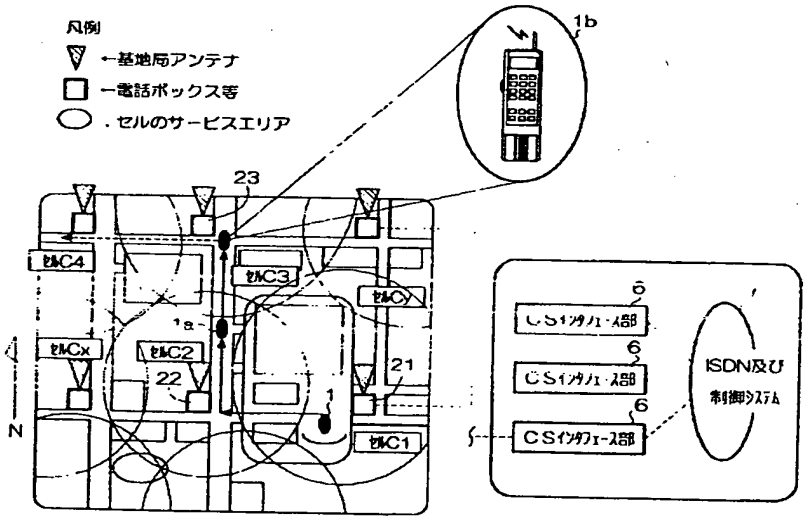
【図３】



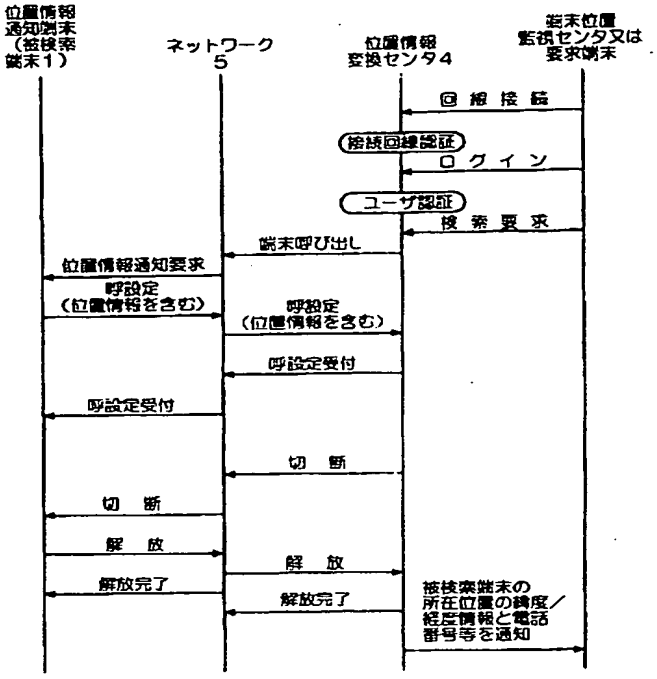
【図４】


位置情報変換センタ
2)情報通知要求
1
3) 基地局ID通知
NTT
CS
ネットワーク
5
4
被検索端末
2
1: 検索要求
4) 緯度経度
情報通知
3
5) 地図表示
位置検索クライアント

【図５】


凡例
←基地局アンテナ
一電話ボックス等
．セルのサービスエリア
1b
23
セルC4
セルC3
セルC
セルCx
セルC2
22
1a
21
1
セルC1
N
6
CSインタフェース部
6
CSインタフェース部
6
CSインタフェース部
ISDN及び
制御システム

【図６】



フロントページの続き

(72)発明者　鈴木　義武
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　西野　豊
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5J062 AA08 BB05 CC14
5K067 AA30 AA35 AA41 BB04 DD17 DD19 DD20 DD23 DD24 EE02 EE10 EE16 FF03 GG01 GG11 HH11 HH22 HH24 HH36 JJ52 JJ54